What is Claimed is:

1. An identity-based-encryption (IBE) signcryption method in which a sender signs and encrypts a message M for a recipient, comprising:

at the sender, digitally signing and encrypting a message M in a signcryption operation using an IBE private key of the sender SK_A and an IBE public key of the recipient ID_B that is based on the recipient's identity to generate a ciphertext C that is a signed and encrypted version of the message M;

sending the ciphertext C to the recipient anonymously, wherein an attacker cannot deduce the authorship of the message from the ciphertext C;

at the recipient, decrypting the ciphertext C using an IBE private key SK_B of the recipient that corresponds to the IBE public key ID_B, wherein decrypting the ciphertext produces an unencrypted version of the message M and an IBE public key of the sender ID_A that corresponds to the IBE private key SK_A; and

at the recipient or at a third party, after the ciphertext has been decrypted by the recipient, performing signature verification in an operation that is separate from the decryption of the ciphertext, wherein performing the signature verification comprises using the decrypted message M and the IBE public key of the sender ID_A to prove that the sender signed the message M.

2. The signcryption method defined in claim 1 wherein digitally signing and encrypting the message M

comprises using the IBE private key SK_A in digitally signing the message M to produce digital signature information and using the IBE private key SK_A in encrypting at least a portion of the digital signature information.

3. The signcryption method defined in claim 2 wherein using the IBE private key SK_A in digitally signing the message M comprises computing a commitment to a secret value and computing a corresponding decommitment.

4. The signcryption method defined in claim 2 wherein using the IBE private key SK_A in encrypting the digital signature information comprises using the IBE private key to compute a symmetric key.

5. The signcryption method defined in claim 4 further comprising using the symmetric key to encrypt the message.

6. The signcryption method defined in claim 4 further comprising using the symmetric key to encrypt the IBE public key of the recipient, at least a portion of the digital signature information, and the message.

7. The signcryption method defined in claim 1 wherein digitally signing and encrypting the message M in the signcryption operation comprises:

computing a commitment to a secret value r and computing a corresponding decommitment;

using the IBE private key SK_A in digitally signing the message M to produce digital signature information; and

using the secret value r in encrypting the message M.

8. The signcryption method defined in claim 7 wherein using the secret value r in encrypting the message M comprises using the secret value r to compute a symmetric key.

9. The signcryption method defined in claim 8 further comprising using the symmetric key to encrypt the message.

10. The signcryption method defined in claim 8 further comprising using the symmetric key to encrypt the IBE public key of the recipient, at least a portion of the digital signature information, and the message.

11. The signcryption method defined in claim 1 wherein digitally signing and encrypting the message M comprises using the IBE private key SK_A in encrypting the message M.

12. The signcryption method defined in claim 1 wherein digitally signing and encrypting the message comprises performing multiplication on an elliptic or hyperelliptic curve.

13. A method of signing and encrypting a

message M comprising:

obtaining an identity-based-encryption (IBE) private key of a user;

using the IBE private key to compute a commitment to a secret value and a corresponding decommitment; and

using a symmetric key that is based on the IBE private key to encrypt at least one of the commitment and the decommitment.

14. The method defined in claim 13 wherein using the symmetric key to encrypt comprises:

concatenating the decommitment and the message; and

using the symmetric key to encrypt the concatenated decommitment and message.

15. The method defined in claim 13 wherein using the symmetric key to encrypt comprises:

concatenating an IBE public key with the message and the decommitment; and

using the symmetric key to encrypt the concatenated IBE public key, decommitment, and message.

16. The method defined in claim 13 wherein computing the decommitment comprises performing multiplication on an elliptic or hyperelliptic curve.

17. The method defined in claim 13 further comprising computing the symmetric key that is based on the IBE private key by performing a bilinear pairing

calculation on an elliptic or hyperelliptic curve.

18. An identity-based-encryption (IBE) signcryption method in which a sender signs and encrypts a message M for an intended recipient, comprising:

at the sender, digitally signing and encrypting a message M in a signcryption operation using an IBE private key of the sender SK_A and an IBE public key of the intended recipient ID_B that is based on the intended recipient's identity to generate a ciphertext C that is a signed and encrypted version of the message M;

sending the ciphertext C to the intended recipient anonymously, wherein an attacker cannot deduce the intended recipient of the message from the ciphertext C;

at the intended recipient, decrypting the ciphertext C using an IBE private key SK_B of the intended recipient that corresponds to the IBE public key ID_B, wherein decrypting the ciphertext produces an unencrypted version of the message M and an IBE public key of the sender ID_A that corresponds to the IBE private key SK_A; and

at the intended recipient or at a third party, after the ciphertext has been decrypted by the intended recipient, performing signature verification in an operation that is separate from the decryption of the ciphertext, wherein performing the signature verification comprises using the decrypted message M and the IBE public key of the sender ID_A to prove that the sender signed the message M.

19. The method defined in claim 18 wherein sending the ciphertext C to the intended recipient anonymously comprises sending the ciphertext C to the intended recipient anonymously such that the attacker cannot deduce the authorship of the message from the ciphertext C.